PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32, G06F 1/00 — A1

(11) International Publication Number: WO 98/07254

(43) International Publication Date: 19 February 1998 (19.02.98)

(21) International Application Number: PCT/GB97/02142

(22) International Filing Date: 8 August 1997 (08.08.97)

(30) Priority Data:
9616737.4 9 August 1996 (09.08.96) GB

(71) Applicant *(for all designated States except US)*: UNIVERSITY COURT OF THE UNIVERSITY OF PAISLEY [GB/GB]; Paisley Campus, High Street, Paisley PA1 2BE (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: CLARK, Douglas, Fraser [GB/GB]; University Court of the University of Paisley, Paisley Campus, High Street, Paisley PA1 2BE (GB). GALBRAITH, Farquhar, Spence [GB/GB]; University Court of the University of Paisley, Paisley Campus, High Street, Paisley PA1 2BE (GB).

(74) Agent: MURGITROYD & COMPANY; 373 Scotland Street, Glasgow G5 8PT (GB).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: DEVICE AND METHOD FOR SAFEGUARDING DATA TRANSFERRED BETWEEN MACHINES OPERATING WITHIN A NETWORK

(57) Abstract

Provision of a secure environment for transferring information in electronic format. Data is encoded before it is sent from a computer to a printer. The software encoding the data simultaneously generates a job specific code. This code must be employed to permit printing of the data.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

DEVICE AND METHOD FOR SAFEGUARDING DATA TRANSFERRED BETWEEN MACHINES OPERATING WITHIN A NETWORK

This invention relates to means for effecting security, and in particular to means for safeguarding data transferred between machines operating within a network environment.

It is recognised that there are numerous situations where although encryption of data prior to its saving in a machine is inappropriate, it is nonetheless desirable that the data is not easily accessible. However when data is transferred between machines within a network there is always the possibility that the data could be picked up from the network link or from a receiving machine.

A practical example would be the printing of a confidential document. If the document is sent from a computer to a printer both of which are networked, there is the possibility that access to the document or a portion thereof may be gained from the network link or the printer server, or from a hard copy when the report has printed.

According to the present invention there is provided

means to safeguard data transferred within a network from data transmitting means to data receiving means comprising:
data transmitting means;
encoding means associated with said data transmitting means;
data receiving means;
decoding means associated with said data receiving means; and
enabling means for the decoding means to allow the data receiving means to utilize transferred data.

Preferably said encoding means includes software which encodes data prior to its transfer from the data transmitting means.

Additionally or alternatively said encoding means may include hardware which encodes data prior to its transfer from the data transmitting means.

Preferably the encoding means includes software which generates the enabling means.

Additionally or alternatively the encoding means may include hardware which generates the enabling means.

Preferably the enabling means is job specific.

Preferably the enabling means is an access code.

Preferably the decoding means is adapted for attachment to the data receiving means. Alternatively the decoding means may be remote from the data receiving means. Alternatively the decoding means may be integrated in the data receiving means.

Preferably the decoding means is a hardware device.

Preferably the decoding means includes means for input of the enabling means.

Preferably the means for input of the enabling means is a data entry device. More preferably the data entry device is a keypad or a swipe.

Preferably said means to safeguard data denies access to transferred data unless the decoding means is enabled by the enabling means within a specified time period from generation of the enabling means.

Preferably said means to safeguard data denies access to transferred data if more than one unsuccessful attempt is made to enable the decoding means.

Preferably the data transmitting means is a computer.

Preferably the data receiving means is a printer.

Alternatively the data receiving means may be a computer.

Alternatively the data receiving means may be a facsimile machine.

Further according to the present invention there is provided a method of safeguarding data transferred within a network from a computer to a printer, comprising the steps of:
providing encoding means in the computer and decoding means for the printer;
encoding the data and generating an access code in the computer;

sending encoded data to the printer; and
applying the access code to the decoding means to enable the decoding means and permit printing of the data.

Preferably the method is applied to an existing network.

Preferably the method is applied to the Internet.

Embodiments of the present invention will now be described by way of example only.

A computer network comprises several client sharing computers and one or several standard laser printer facilities connected to a server. Data is generated and saved on the computer prior to the generation of a physical report.

To generate a report, data is sent to a printer either directly or through a printer server. When a computer user instructs the printing of particular data, encoding means in the form of software encodes the data. This software, which may be included in the printer driver software, intercepts unencoded output from a printer driver and encodes the information before sending it to the printer server. In addition, the software generates and displays enabling means for each print job in the form of a job specific access code. Thus the codes generated by the encoder software form part of an encryption algorithm used in the coding and decoding processes.

The data is sent over the network in the encoded form. This ensures that any data picked up from the network link, arriving at other than its designated address, or

stored on the printer server, is incomprehensible.

Decoding means controls the flow of data. The decoding means incorporates a keypad and prevents decoding of any data received by the decoding means unless the correct code is entered in the keypad. A standard laser printer has a port to accommodate memory and/or font cartridges. Decoding means in the form of a cartridge with the facility to register a code is plugged into this port.

Alternatively discrete decoding means is inserted between the computer or printer server and the printer. This discrete decoding means may take the form of a box including electronics, connectors and power switches. Alternatively the electronics are incorporated on a single chip and included in a printer cable - that is, the decoding means is integrated in the printer cable. The above options allow for the adaption of an existing printer. The decoding means can be integrated in new printers.

The decoding means comprises a microcontroller or microprocessor or other programmable device which controls the flow of data in both encrypted and non-encrypted format between the computer and the printer. The decoding means further includes ancillary electronics. These ancillary electronics include voltage stabilisation circuitry and buffering between the decoding means and the computer and printer. External features include an LCD display, a code input device such as a keypad, connectors and power switches. The processor controls the display output and the keypad input, when it is necessary to enter the code. When the correct code has been entered, the controller also performs the decryption of the incoming data.

An intelligible output is obtainable only when the correct code is entered in the decoding means. The code is job specific and the decoding means can be programmed to delete a print job, or store it temporarily, or return it to the print server, unless the correct job code is entered within a specified time period from the print job being sent to the printer from the print server, or if the wrong code is entered more than once.

The advantages of this invention include its simplicity. Its inclusion in an existing network environment requires minimal adaptation of that network. In essence all that is required is a code-operated cartridge adapted for attachment to existing printers or a stand alone box, and suitable software.

The software can be part of a printer driver or an addition to the printer driver. When the printer driver has coded the job for a specific printer, the encryption driver intercepts this information before sending it to the printer. The software algorithm is platform and network independent, and runs on a variety of platforms such as Windows™ or OS/2™, and networks such as Novell™.

Since the information is sent to the printer in encoded format it cannot be picked up from the network link in intelligible form. Information stored on the printer server is encoded and lost printouts are incomprehensible. Thus confidential reports or the like sent to a network printer from a computer or over the Internet may be accessed only by the initiator of the print job or someone authorised by them.

Access may similarly be denied to confidential

information sent from computer to computer or computer to facsimile machine . The invention also facilitates monitoring and/or restricting use of a printer.

Modifications and improvements may be made to the above without departing from the scope of the invention.

CLAIMS

1. Means to safeguard data transferred within a network from data transmitting means to data receiving means comprising:
data transmitting means;
encoding means associated with said data transmitting means;
data receiving means;
decoding means associated with said data receiving means; and
enabling means for the decoding means to allow the data receiving means to utilize transferred data.

2. Means to safeguard data as claimed in Claim 1 wherein the encoding means includes software which encodes data prior to its transfer from the data transmitting means.

3. Means to safeguard data as claimed in any preceding claim wherein the encoding means includes hardware which encodes data prior to its transfer from the data transmitting means.

4. Means to safeguard data as claimed in any preceding claim wherein the encoding means includes software which generates the enabling means.

5. Means to safeguard data as claimed in any preceding claim wherein the encoding means includes hardware which generates the enabling means.

6. Means to safeguard data as claimed in any preceding claim wherein the enabling means is job

specific.

7. Means to safeguard data as claimed in any preceding claim wherein the enabling means is an access code.

8. Means to safeguard data as claimed in any preceding claim wherein the decoding means is adapted for attachment to the data receiving means.

9. Means to safeguard data as claimed in any preceding claim wherein the decoding means is remote from the data receiving means.

10. Means to safeguard data as claimed in any preceding claim wherein the decoding means is integrated in the data receiving means.

11. Means to safeguard data as claimed in any preceding claim wherein the decoding means is a hardware device.

12. Means to safeguard data as claimed in any preceding claim wherein the decoding means includes means for input of the enabling means.

13. Means to safeguard data as claimed in Claim 12 wherein the means for input of the enabling means is a data entry device.

14. Means to safeguard data as claimed in Claim 13 wherein the data entry device is a keypad or a swipe.

15. Means to safeguard data as claimed in any

preceding claim which denies access to transferred data unless the decoding means is enabled by the enabling means within a specified time period from generation of the enabling means.

16. Means to safeguard data as claimed in any preceding claim which denies access to transferred data if more than one unsuccessful attempt is made to enable the decoding means.

17. Means to safeguard data as claimed in any preceding claim wherein the data transmitting means is a computer.

18. Means to safeguard data as claimed in any preceding claim wherein the data receiving means is a printer.

19. Means to safeguard data as claimed in Claims 1 to 19 wherein the data receiving means is a computer.

20. Means to safeguard data as claimed in Claims 1 to 19 wherein the data receiving means is a facsimile machine.

21. A method of safeguarding data transferred within a network from a computer to a printer comprising the steps of:
providing encoding means in the computer and decoding means for the printer;
encoding the data and generating an access code in the computer;
sending encoded data to the printer; and
applying the access code to the decoding means to enable the decoding means and permit printing of the data.

22. A method of safeguarding data as claimed in Claim 21 applied to an existing network.

23. A method of safeguarding data as claimed in Claim 21 applied to the Internet.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 97/02142

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32 G06F1/00

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 445 290 A (SECOM CO LTD) 11 September 1991 see page 2, line 3 - line 6 see page 4, line 9 - line 15 see page 5, line 35 - line 43 see page 5, line 47 - line 57 see page 6, line 31 - line 56	1,3,5,6, 8,11,15
A	---	20
X	EP 0 665 486 A (AT & T CORP) 2 August 1995 see column 1, line 34 - column 2, line 5 see column 3, line 6 - line 27 see column 4, line 13 - line 32 see column 5, line 12 - line 27 see column 6, line 35 - line 56 see column 7, line 43 - line 58	1,4-6, 17-23
	--- -/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 November 1997	02/12/1997

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Larcinese, A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter. .onal Application No
PCT/GB 97/02142

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	GB 2 188 758 A (BERTENSHAW PHILIP HALL;JONES JOHN; SEDGWICK ANTHONY) 7 October 1987 see page 1, left-hand column, line 15 - line 17 see page 1, left-hand column, line 41 - line 57 see page 1, right-hand column, line 82 - line 87 see page 1, right-hand column, line 96 - line 108 see page 1, right-hand column, line 116 - line 125 see page 2, right-hand column, line 90 - page 3, left-hand column, line 14	21-23

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 97/02142

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0445290 A	11-09-91	JP 2134940 A	23-05-90
		AT 149769 T	15-03-97
		CA 1337997 A	23-01-96
		DE 68927831 D	10-04-97
		DE 68927831 T	25-09-97
		WO 9006029 A	31-05-90
		KR 9400178 B	08-01-94
		US 5253293 A	12-10-93
EP 0665486 A	02-08-95	US 5509074 A	16-04-96
		CA 2137065 A	28-07-95
		JP 7239828 A	12-09-95
GB 2188758 A	07-10-87	NONE	